

## **REMARKS**

Applicant respectfully requests reconsideration and allowance of the subject application in view of the foregoing amendments and the following remarks.

Claims 1-23 are pending in the application, with Claims 1, 5, 7, 17, and 20 being independent. Applicant amends independent Claims 1, 5, 7, 17, and 20 to clarify claimed subject matter and/or correct informalities. The original specification and drawings support these claim amendments at least at pages 4, 5, 6, 8, and in Figures 4 and 6. Therefore, these revisions introduce no new matter.

### **Claim Rejections 35 U.S.C. §112, Second Paragraph**

Claims 1-4 and 6 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Without conceding the propriety of the rejection, Applicant amends **Claim 1** to clarify the subject matter. In the telephonic conference, Examiner Whipple tentatively agrees that the amendment overcomes the §112 rejection. Dependent Claims 2-4 and 6 depend from independent Claim 1, and are allowable by virtue of this dependency.

Applicant respectfully submits that these claims comply with 35 U.S.C. §112, second paragraph and as a result the rejections are now moot. Applicant respectfully requests that the §112 rejections be withdrawn.

**Claim Rejections 35 U.S.C. §103: A. and B.**

A. Claims 1, 3-10, and 13-23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,092,196 (Reiche) in view of U.S. Patent No. 6,199,113 (Alegre), further in view of U.S. Patent No. 6,715,080 (Starkovich), and further in view of what was well known in the art. Applicant respectfully traverses the rejection.

Without conceding the propriety of the stated rejections, and only to advance the prosecution of this application, Applicant amends **Independent Claim 1**, to clarify further features of the subject matter. Amended Claim 1 now recites:

A method implemented on a computing device by a processor configured to execute instructions that, when executed by the processor, for seeking access to a first server, the method comprising:

determining that a client seeking access to the first server is not authenticated by an authentication server;

communicating a request for login information to be returned to the authentication server from the client;

receiving the first login information at the authentication server from the client;

associating the login information with a user profile information;

authenticating the client by comparing the login information with authentication information maintained by the authentication server;

when the login information matches the authentication information,

generating a user authentication indicator at the authentication server;

sending the user authentication indicator to the first server; and

sending the user profile information associated with the login information to the first server;

at a time:

after sending the user authentication indicator to the first server;

determining that the client seeking access to the first server is not authenticated by the authentication server;

communicating a request for an other login information to be returned to the authentication server from the client;

receiving the other login information at the authentication server from the client;

associating the other login information with the user profile information;

authenticating the client by comparing the other login information with the authentication information maintained by the authentication server; when the other login information does not match the authentication information,

generating an other user authentication indicator at the authentication server;

sending the other user authentication indicator to the first server;

**when the other login information matches the authentication information, and**

**copying cookies to the client, redirecting a browser to an affiliate server, and indicated a period of time for the cookies to be valid, wherein the cookies are encrypted using a key unique to the affiliate server.**

Applicant respectfully submits that Reiche, Alegre, and/or Starkovich, alone or in combination, fail to disclose, teach, or suggest such a method.

**References Fail to Disclose, Teach, or Suggest Features of Claim 1**

First, Applicant asserts the Office no longer establishes a *prima facie* case of obviousness. As discussed during the telephonic interview, Reiche, Alegre, and/or Starkovich, alone or in combination, fail to disclose, teach, or suggest the features of Applicant's amended Claim 1.

Second, Applicant submits that Reiche fails to disclose, teach, or suggest "sending a user profile information associated with the login information to the first server". Reiche is directed towards privacy, authentication, and access control (Col. 1, lines 7-8). An HTTP distributed remote user authentication system in Reiche provides for data network implementation of an improved user access control protocol (Col. 4, lines 22-23).

Third, Applicant submits that Alegre fails to compensate for the deficiencies of Reiche. Alegre uses an authentication database to authenticate the user, a session key is created and stored at the browser (Abstract). Alegre is directed towards authenticating a user for allowing access to resources on a trusted network (Col. 1, lines 9-10). If UID and

PWD are authenticated in Alegre (step 714: YES), login process 512 receives a session key and user profile from authentication server 226 (Col. 6, lines 17-19). Thus, Alegre does not provide what is missing from Reiche to support a §103 rejection.

Fourth, Applicant submits that Starkovich fails to remedy the deficiencies of Reiche and/or Alegre, alone or in combination. Starkovich is directed towards the interchange of Cookie information and standard Common Gateway Interface (CGI) variables between a user system and an On-Line Transaction Processing (OLTP) enterprise server (Abstract). While Starkovich mentions SGate will write authentication information to a Cookie that is used on subsequent requests to save the user the hassle of repeatedly inputting authentication information, this is not the same as Applicant's feature.

Applicant submits that Reiche, Alegre, and/or Starkovich, alone or in combination, fail to disclose, teach, or suggest "*when the other login information matches the authentication information, copying cookies to the client, redirecting a browser to an affiliate server, and indicated a period of time for the cookies to be valid, wherein the cookies are encrypted using a key unique to the affiliate server*", as recited in Applicant's amended Claim 1. Accordingly, Applicant submits that the evidence relied upon by the Office no longer supports the rejections made under §103(a).

**Independent Claims 5, 7, 17, and 20** are directed to a computer-readable storage media, a method, a computer-readable storage media, and a system, respectively, and each is allowable for reasons similar to those discussed above with respect to Claim 1.

**Independent Claim 5** recites:

One or more computer-readable storage media having stored thereon a plurality of instructions that when executed by a processor, the plurality of instructions comprising:

determining that a client seeking access to a first server is not authenticated by an authentication server;

communicating a request for a login information to be returned to the authentication server from the client;

receiving the login information at the authentication server from the client; authenticating the client by comparing the login information with authentication information maintained by the authentication server;

associating login information with a user profile information, the user profile information allows a user to enter the user profile information once and continue to use the user profile information during subsequent logins;

when the login information does not match the authentication information,

generating a user authentication indicator at the authentication server;

sending the user authentication indicator to the first server; and

sending user profile information associated with the client login information to the first server; and

**when the other login information matches the authentication information,**

**copying cookies to the client, redirecting a browser to an affiliate server, and indicated a period of time for the cookies to be valid, wherein the cookies are encrypted using a key unique to the affiliate server.**

Applicant respectfully submits that Reiche, Alegre, and/or Starkovich, alone or in combination, fail to disclose, teach, or suggest such a method.

**Independent Claim 7** recites:

A method implemented on a computing device by a processor configured to execute instructions that, when executed by the processor, of authenticating a client with respect to a network server to which the client is seeking access, the method comprising:

receiving a request at an authentication server from the network server to authenticate a client;

determining that the client is not authenticated by the authentication server;

registering a user profile information with the authentication server, the user profile information allows a user to enter the user profile information once and continue to use the user profile information during subsequent logins;

receiving login information at the authentication server from the client;

authenticating the client at the authentication server by comparing the received login information with authentication information maintained by the authentication server; and

determining that the received login information does not match the authentication information;

generating an authentication indication at the authentication server;

communicating the authentication information and the user profile information associated with the client login information to the network server; and

**when the other login information matches the authentication information,**

**copying cookies to the client, redirecting a browser to an affiliate server, and indicated a period of time for the cookies to be valid, wherein the cookies are encrypted using a key unique to the affiliate server.**

Applicant respectfully submits that Reiche, Alegre, and/or Starkovich, alone or in combination, fail to disclose, teach, or suggest such a method.

**Independent Claim 17 recites:**

One or more computer-readable storage media having stored thereon a plurality of instructions that when executed by a processor, the plurality of instructions comprising:

receiving a request to authenticate a user seeking access to a network server;

determining that the user is not authenticated by an authentication server;

registering a user profile information with the authentication server, the user profile information allows a user to enter the user profile information once and continue to use the user profile information during subsequent logins;

receiving login information at the authentication server from the user;

authenticating the user at the authentication server by comparing the received login information with authentication information maintained by the authentication server;

when the received login information does not match the authentication information,

generating a user authentication indicator at the authentication server;

sending the user authentication indicator to the network server; and

sending the user profile information associated with the login information to the network server; and

**when the other login information matches the authentication information,**

**copying cookies to the client, redirecting a browser to an affiliate server, and indicated a period of time for the cookies to be valid, wherein the cookies are encrypted using a key unique to the affiliate server.**

Applicant respectfully submits that Reiche, Alegre, and/or Starkovich, alone or in combination, fail to disclose, teach, or suggest such a computer-readable storage medium.

**Independent Claim 20** recites:

A system comprising:

a network server to receive a request by a client to gain access to the network server,

the network server to transmit a request to the authentication server for the authentication server to authenticate the client, wherein the request includes a client login information;

an authentication server to determine that the client is authenticated with respect to the authentication server,

an authentication database identifying elements of a user profile information provided to the authentication server, the user profile information allows a user to enter the user profile information once and continue to use the user profile information during subsequent logins;

the authentication server to transmit a client authentication indicator to the network server, wherein the client authentication indicator to indicate whether the client is authenticated;

whereby the network server is to grant access to the client at the network server, wherein the network server is to receive a user profile information associated with the client login information when the client

authentication indicator determines that the client is authenticated at the authentication server;

when the received login information does not match the authentication information,

generating a user authentication indicator at the authentication server;

sending the user authentication indicator to the network server; and

sending the user profile information associated with the login information to the network server; and

when the other login information matches the authentication information,

copying cookies to the client, redirecting a browser to an affiliate server, and indicated a period of time for the cookies to be valid, wherein the cookies are encrypted using a key unique to the affiliate server.

Applicant respectfully submits that Reiche, Alegre, and/or Starkovich, alone or in combination, fail to disclose, teach, or suggest such a system.

**Dependent Claims 2-4, 6, 8-16, 18-19, and 21-23** depend directly or indirectly from one of independent Claims 1, 7, 17, and 20, respectively, and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features that, in combination with those recited in Claim 1, are not disclosed, taught, or suggested by Reiche, Alegre, and/or Starkovich, alone or in combination.

Applicant respectfully submits that the cited references do not render the claimed subject matter obvious and that the claimed subject matter, therefore, patentably distinguishes over the cited references. For all of these reasons, Applicant respectfully requests the §103(a) rejection of these claims should be withdrawn.

**B. Claims 2 and 11-12 stand rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 6,092,196 (Reiche), U.S. Patent No. 6,199,113 (Alegre), U.S. Patent No. 6,715,080 (Starkovich) and further in view of U.S. Patent No. 5,418,854 (Kaufman). Applicant respectfully traverses the rejection.**

As explained above with respect to the rejection under 35 U.S.C. §103(a), Applicant asserts that Reiche, Alegre, and/or Starkovich, alone or in combination, fail to disclose, teach, or suggest the features of independent Claims 1 and 7. **Dependent Claims 2 and 11-12** depend directly or indirectly from one of independent Claims 1 and 7, respectively, and are allowable by virtue of this dependency. These dependent claims are also allowable for their own recited features that, in combination with those recited in Claims 1 and 7, are not disclosed, taught, or suggested by Reiche, Alegre, and/or Starkovich, alone or in combination.

The Office stated Reiche does not mention “on the indicator does not contain reference to the login information” (Office Action, pg. 11). Applicant agrees with this assessment.

However, Kaufman fails to compensate for the deficiencies of Reiche. Kaufman was cited for its alleged teaching of a “user authentication indicator [that] does not contain reference of the login information” (Office Action, pg. 11). For example, Kaufman fails to teach or suggest “sending user profile information associated with the client login information to the first server,” as in Applicant’s amended Claim 1.

**Dependent Claim 2** depends from Claim 1 and, therefore, is allowable by virtue of its dependence from independent Claim 1, as well as for the additional features that it recites.

## **Claims 11 and 12**

Without conceding the propriety of the stated rejections, and only to advance the prosecution of this application, Applicant amends **Independent Claim 7**, to clarify further features of the subject matter. Amended Claim 7 now recites:

A method implemented on a computing device by a processor configured to execute instructions that, when executed by the processor, of authenticating a client with respect to a network server to which the client is seeking access, the method comprising:

receiving a request at an authentication server from the network server to authenticate a client;

determining that the client is not authenticated by the authentication server;

registering a user profile information with the authentication server, the user profile information allows a user to enter the user profile information once and continue to use the user profile information during subsequent logins;

receiving login information at the authentication server from the client;

authenticating the client at the authentication server by comparing the received login information with authentication information maintained by the authentication server; and

determining that the received login information does not match the authentication information;

generating an authentication indication at the authentication server;

communicating the authentication information and the user profile information associated with the client login information to the network server; and

**when the other login information matches the authentication information,**

**copying cookies to the client, redirecting a browser to an affiliate server, and indicated a period of time for the cookies to be valid, wherein the cookies are encrypted using a key unique to the affiliate server.**

Applicant respectfully submits that no such method is disclosed, taught, or suggested by Reiche, Alegre, and/or Starkovich, and/or Kaufman, alone or in combination.

**Dependent Claims 11 and 12** depend from independent Claim 7. Reiche, Alegre, and/or Starkovich do not disclose, teach, or suggest every element of Applicant's amended Claim 7. For example, Reiche, Alegre, and/or Starkovich do not disclose, teach, or suggest “*when the other login information matches the authentication information, and copying cookies to the client, redirecting a browser to an affiliate server, and indicated a period of time for the cookies to be valid, wherein the cookies are encrypted using a key unique to the affiliate server*” as recited in Applicant's amended Claim 7.

The Kaufman document does not compensate for the deficiencies of Reiche, Alegre, and/or Starkovich, described above with respect to Claim 7. Therefore, Applicant respectfully submits amended independent Claim 7 is not obvious in view of these references. Claims 11 and 12 depend from Claim 7, and, therefore, are allowable by virtue of their dependence from independent Claim 7, as well as for the additional features that each claim recites.

Applicant respectfully submits that the cited references do not render the claimed subject matter obvious and that the claimed subject matter, therefore, patentably distinguishes over the cited references. For all of these reasons, Applicant respectfully requests the §103(a) rejection of these claims should be withdrawn.

**CONCLUSION**

Claims 1-23 are in condition for allowance. Applicant respectfully requests reconsideration and prompt allowance of the subject application. If any issue remains unresolved that would prevent allowance of this case, the Office is requested to contact the undersigned attorney to resolve the issue.

Respectfully Submitted,

Lee & Hayes, PLLC  
601 W. Riverside Avenue, Suite 1400  
Spokane, WA 99201

Dated: 3-9-2009

By: Shirley Lee Anderson  
Shirley Lee Anderson  
Reg. No. 57,763  
509.944.4758